AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

Claims 1 – 23 (Canceled)

24. (New) A countermeasure method in an electronic component that implements the DES cryptographic algorithm in which multiple rounds of calculation are performed on input data, wherein each round of calculation includes at least the following operations:

a first permutation of data;

manipulation of the permuted data by a secret key;

a table look-up operation based on the manipulated data; and

a second permutation of data;

wherein, for a plurality of successive rounds of said algorithm, at least one of said first and second permutations of data comprises the following steps:

selecting a first random value having the same size as the data being permuted,

performing an exclusive-OR operation between the data being permuted and the first random value to generate a second random value,

executing said permutation operation on each of the first and second random values, to generate respective first and second random results, and

performing an exclusive-OR operation between said first and second random results to produce a final permuted result.

25. (New) The method of claim 24, wherein said steps are performed for both of said first and second permutation operations in each of said plurality of successive rounds.

26. (New) The method of claim 25, wherein the first and second permutation operations utilize different respective first random values.

27. (New) The method of claim 24, wherein said plurality of successive rounds comprise only the first three and last three rounds of said algorithm.

28. (New) The method of claim 24, wherein the manipulation operation performed during said plurality of successive rounds comprises the following steps:

performing an exclusive-OR operation between said secret key and a third random value having the same size as said key, to generate a fourth random value;

performing bit-by-bit operations on each of said third and fourth random values to produce a pair of intermediate keys;

manipulating the result of said first permutation operation with one of said intermediate keys to produce an intermediate result, and

manipulating said intermediate result with the other of said intermediate keys to produce an output data item.

29. (New) The method of claim 28 wherein said manipulating steps comprise exclusive-OR operations.

30. (New) The method of claim 28 wherein said bit-by-bit operations comprise a key permutation operation, a shift operation and a compression permutation operation.

31. (New) An electronic component that implements the DES cryptographic algorithm in which multiple rounds of calculation are performed on input data, said electronic component including a microprocessor that executes the following operations during each round of calculation:

a first permutation of data;

manipulation of the permuted data by a secret key;

a table look-up operation based on the manipulated data; and

a second permutation of data;

wherein, for a plurality of successive rounds of said algorithm, said microprocessor executes the following steps for at least one of said first and second permutations of data:

selecting a first random value having the same size as the data being permuted,

performing an exclusive-OR operation between the data being permuted and the first random value to generate a second random value,

executing said permutation operation on each of the first and second random values, to generate respective first and second random results, and

performing an exclusive-OR operation between said first and second random results to produce a final permuted result.

32. (New) The electronic component of claim 31, wherein said steps are executed for both of said first and second permutation operations in each of said plurality of successive rounds.

33. (New) The electronic component of claim 32, wherein said microprocessor selects different first random values for the first and second permutation operations, respectively.

34. (New) The electronic component of claim 31, wherein said plurality of successive rounds comprise only the first three and last three rounds of said algorithm.

35. (New) The electronic component of claim 31, wherein the manipulation operation executed by said microprocessor during said plurality of successive rounds comprises the following steps:

performing an exclusive-OR operation between said secret key and a third random value having the same size as said key, to generate a fourth random value;

performing bit-by-bit operations on each of said third and fourth random values to produce a pair of intermediate keys;

manipulating the result of said first permutation operation with one of said intermediate keys to produce an intermediate result, and

manipulating said intermediate result with the other of said intermediate keys to produce an output data item.

36. (New) The electronic component of claim 35 wherein said manipulating steps comprise exclusive-OR operations.

37. (New) The electronic component of claim 35 wherein said bit-by-bit operations comprise a key permutation operation, a shift operation and a compression permutation operation.